CLAIMS

1. A remote access system comprising

a server,

a client apparatus for accessing said server,

a network for connecting said server and said client apparatus, and

a storage medium being connected to said client apparatus and storing a remote manipulation application for remotely manipulating said server, an encryption application for encrypting communications on said network, a job application, and an authentication information for remote manipulation to said server stored in the anti-tampering storage area,

wherein

said storage medium stores a middleware for operating said remote manipulation application, said encryption application, and said job application in said client apparatus, and

a CPU of said client apparatus operates the application interface for file access and driver for file access when it executes said middleware for the file access and also operates the interface handler and device driver when it executes the authentication process in view of thereby making communications between said server and said client apparatus.

2. The remote access system according to claim 1, wherein when an instruction is generated from said driver for file access or from said device driver, said

instruction is controlled in the predetermined sequence.

3. The remote access system according to claim 2, wherein when an instruction is generated from said driver for file access or from said device driver, the instruction from said device driver is executed preferentially.

4. The remote access system according to claim 1, wherein said storage medium further includes a temporary storage area, and the data generated by the process executed by said client apparatus is stored to said temporary storage area.

5. A remote access system comprising

a server,

a gateway connected to said server,

a client apparatus for executing the authentication process for said gateway by making accessing to said server,

a network for connecting said server and said client apparatus, and

a storage medium being connected to said client apparatus and storing a remote manipulation application for remotely manipulating said server, an encryption application for encrypting communications on said network, a job application, and an authentication information for remote manipulation to said server stored in the anti-tampering storage area,

wherein

said storage medium stores a middleware for operating said remote manipulation application, said encryption application, and said job application in said client apparatus, and

a CPU of said client apparatus operates the application interface for file access and driver for file access when it executes said middleware for the file access and also operates the interface handler and device driver when it executes the authentication process in view of thereby making communications between said server and said client apparatus.

6. The remote access system according to claim 1,

wherein

said server includes a plurality of servers and a controller connected to a plurality of said servers, and

said client apparatus makes access to said controller for management of power supply of a plurality of said servers.

7. The remote access system according to claim 1, wherein said storage medium holds a copy of the authentication information stored within an anti-tampering area.

8. A gateway in a remote access system for making access to said server from said client apparatus, comprising

a server,

a client apparatus for making access to said server,

a storage medium storing

a remote manipulation application program connected to said client apparatus for remote manipulation of said server,

an encryption application program for encryption of the communications on said network, and

the authentication information for remote manipulation for said server stored in an anti-tampering storage area,

wherein

the authentication process of a user manipulating said client apparatus is conducted on the basis of said authentication information transmitted via the interface handler and the device driver which is operated with the middleware loaded to said client apparatus from said storage medium.

9. A client apparatus connected to a server via a network, comprising

a reader/writer connected to a storage medium storing a remote manipulation application program for remote manipulation of said server, an encryption application program for encrypting communications on said network, and an authentication information for remote manipulation for said server stored in an anti-tampering storing area,

wherein

in order to execute the file access, the communications with said server are executed by operating the application interface for file access and the driver for file access when the middleware loaded from said storage medium is executed via said reader/writer and

in order to conduct the authentication process, the communications with said server are executed by operating the interface handler and the device driver.

10. A program for remote access to the client apparatus for making access to said server via a server and a network,

wherein

when the same program is installed to said client apparatus for the file access, communications between said server and said client apparatus may be realized by operating the application interface for file access and the driver for file access, and

when the authentication process is executed, communications between said server and said client apparatus may be realized by operating the interface handler and the device driver.

11. A remote access system comprising

a server,

a client apparatus for making access to said server via a network, and

a storage medium connected to said client

apparatus for storing a remote manipulation application program for remote manipulation of said server, an encryption application program for encrypting communications on said network, a job application, an authentication information for remote manipulation to said server stored in an anti-tampering storing area, a boot program executed by the BIOS of said client apparatus when said client apparatus is driven, and an OS program,

wherein

BIOS of said client apparatus is set to detect the boot program stored in said storage medium earlier than the boot program in said client apparatus, and

said client apparatus detects, after the power supply is turned ON, the boot program stored in said storage medium and the OS program stored in said storage medium is acquired and executed with said boot program.

12. The remote access system according to claim 11, wherein

said client apparatus includes a display means, and

after said OS program is driven and said remote manipulation application is executed, a communication authentication request for said server is displayed first on said display means.

13. The remote access system according to claim

11,

wherein

said storage medium includes a means for selecting whether said OS program is driven or not on said client apparatus,

when it is selected that said OS program is driven on said client apparatus with said means for selection, said OS program is executed which is stored in said storage medium on said client apparatus by transmitting the boot program on said storage medium to said client apparatus, and

when it is selected that said OS program is not driven on said client apparatus with said means for selection, the OS program is executed which is previously stored in said client apparatus on said client apparatus by transmitting a dummy data to said client apparatus.

14. The remote access system according to claim 11,

wherein

said storage medium is connected to said client apparatus via the reader/writer of said storage medium,

said reader/writer includes a means for selecting whether said OS program is driven on said client apparatus or not,

when it is selected that said OS program is driven on said client apparatus with said means for

selection, the OS program stored on said storage medium is executed on said client apparatus by transmitting the boot program on said storage medium to said client apparatus, and

when it is selected that said OS program is not driven on said client apparatus with said means for selection, the OS program stored previously to said client apparatus is executed on said client apparatus by transmitting a dummy data to said client apparatus.

15. The remote access system according to claim 13,

wherein

the boot program stored in said storage medium decides, after it is stored in said client apparatus, whether a storage device provided in said client apparatus is restricted in access or not, and

when access is restricted, said access restriction is cancelled using the authentication information stored in said storage medium to execute the OS program stored in said storage medium.

16. The remote access system according to claim 15, wherein said boot program executes the OS program stored in said storage medium, if cancellation of said access restriction using the authentication information stored in said storage medium has failed.

17. A storage medium connected to a client apparatus accessed to a server via a network, storing

a remote manipulation application program for

remote manipulation of said server,

an encryption application program for encryption of communications on said network,

a job application,

an authentication information for remote manipulation for said server stored in an anti-tampering storing area,

a boot program executed by the BIOS of said client apparatus when said client apparatus is driven, and

an OS program,

wherein

the BIOS of said client apparatus is set to detect the boot program stored in said storage medium earlier than the boot program in said client apparatus, the boot program stored in said storage medium is detected with said BIOS after the power supply of said client apparatus is turned ON, and the OS program stored in said storage medium is transmitted to said client apparatus with said boot program.

18. The storage medium according to claim 17, comprising

means for selecting whether said OS program is driven on said client apparatus or not,

wherein

when it is selected that said OS program is driven on said client apparatus with said means for selection, said OS program is executed on said client

apparatus by transmitting said boot program to said client apparatus, and

when it is selected that said OS program is driven on said client apparatus with said means for selection, the OS program previously stored in said client apparatus is executed on said client apparatus by transmitting a dummy data to said client apparatus.

19. The storage medium according to claim 17, wherein

the boot program stored in said storage medium decides, after it is stored to said client apparatus, whether the storage device provided in said client apparatus is restricted in access or not, and wherein

when access is restricted, the authentication information stored in said storage medium is transmitted to said client apparatus in order to cancel said access restriction and the OS program stored in said storage medium is executed.

20. The storage medium according to claim 19, wherein

when cancellation of said access restriction using the authentication information stored in said storage medium has failed, said boot program controls said client apparatus to execute the OS program stored in said storage medium.

21. The storage medium according to claim 18, wherein

said storage medium includes a reader/writer connected to aid client apparatus and

said means for selection is provided in the side of said reader/writer.